

UNCLASSIFIED



DoD Public Key Enablement (PKE) Reference Guide

Configuring Firefox to Utilize the DoD CAC

Contact: [dodpke@mail.mil](mailto:dodpke@mail.mil)

URL: <http://iase.disa.mil/pki-pke>

Enabling PKI Technology  
for DoD users

# Configuring Firefox to Utilize the DoD CAC

16 September 2013

Version 1.6

DOD PKE Team

UNCLASSIFIED

## Revision History

Issue Date	Revision	Change Description
1/18/10	1.0	Initial Document Creation
3/5/10	1.1	Updated Document to comply with new QRG format
6/10/10	1.2	Updated to include OCSP Fails->Treat as Invalid
9/20/11	1.3	Updated to add Firefox version information, reflect InstallRoot 3.15, and updated DoD PKE website URL
1/17/12	1.4	Added ActivClient 6.2 acpkcs211.dll path information and removed extra instructions for InstallRoot 3.13 and earlier.
8/16/12	1.5	Updated DoD PKE support email address
9/16/13	1.6	Updated ActivClient 6.2 path with 32 bit path.

# Contents

<b>INTRODUCTION .....</b>	<b>1</b>
PURPOSE.....	1
SCOPE .....	1
<b>INSTALL CERTIFICATES FROM INSTALLROOT .....</b>	<b>2</b>
<b>USING COMMON ACCESS CARD (CAC) CERTIFICATES IN FIREFOX.....</b>	<b>3</b>
<b>ENSURE THE ONLINE CERTIFICATE STATUS PROTOCOL (OCSP) IS PERFORMING REVOCATION CHECKING .....</b>	<b>6</b>
<b>APPENDIX A: SUPPLEMENTAL INFORMATION.....</b>	<b>8</b>

## Introduction

The DoD Public Key Enablement (PKE) Reference Guides (RGs) are developed to help an organization augment their security posture through the use of the DoD Public Key Infrastructure (PKI). The PKE RGs contain procedures for enabling products and associated technologies to leverage the security services offered by the DoD PKI.

### Purpose

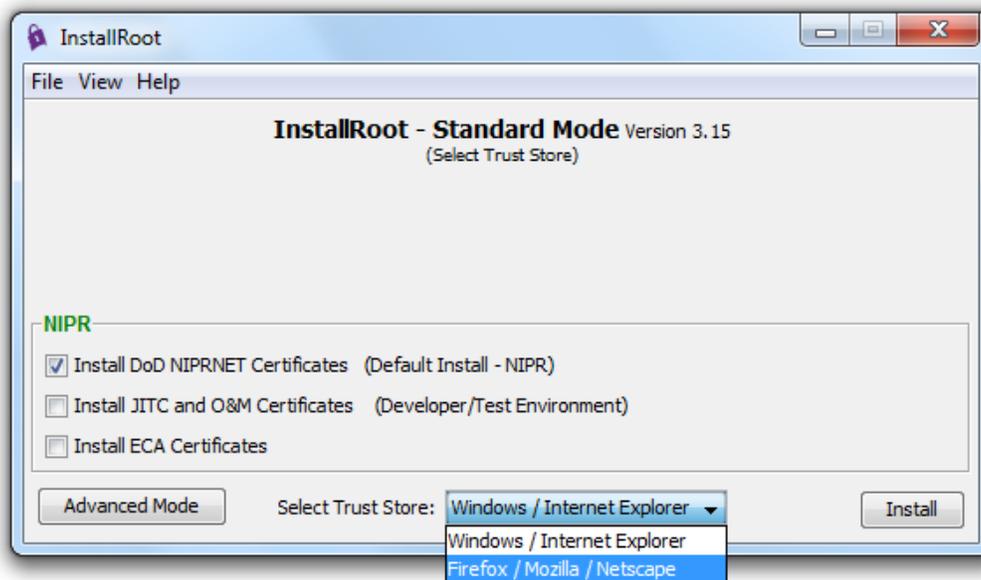
The goal of this RG is to aid in enabling Firefox version 3.6 on Windows operating systems for use with DoD websites. Contained in this document are instructions to install the DoD PKI Certification Authority (CA) certificates, use the Common Access Card (CAC) with Firefox, and configure certificate validation for Firefox. The overall goal is to PK-enable Firefox.

### Scope

This document is intended for all users of PKI technologies. No in-depth knowledge of PKI is required, and no intimate knowledge of CACs is necessary. Some experience installing and configuring software on the Windows platforms is helpful when reading this guide.

## Install Certificates from InstallRoot

- 1) Download and install the InstallRoot tool following the instructions in the InstallRoot User Guide. InstallRoot may be downloaded from <http://iase.disa.mil/pki-pke> under Tools > Trust Store Management.
- 2) Open the InstallRoot tool and select **Firefox/Mozilla/Netscape** from the **Select Trust Store** picklist at the bottom of the window.
- 3) Ensure only the top **Install DoD NIRPNET Certificates** box is checked.



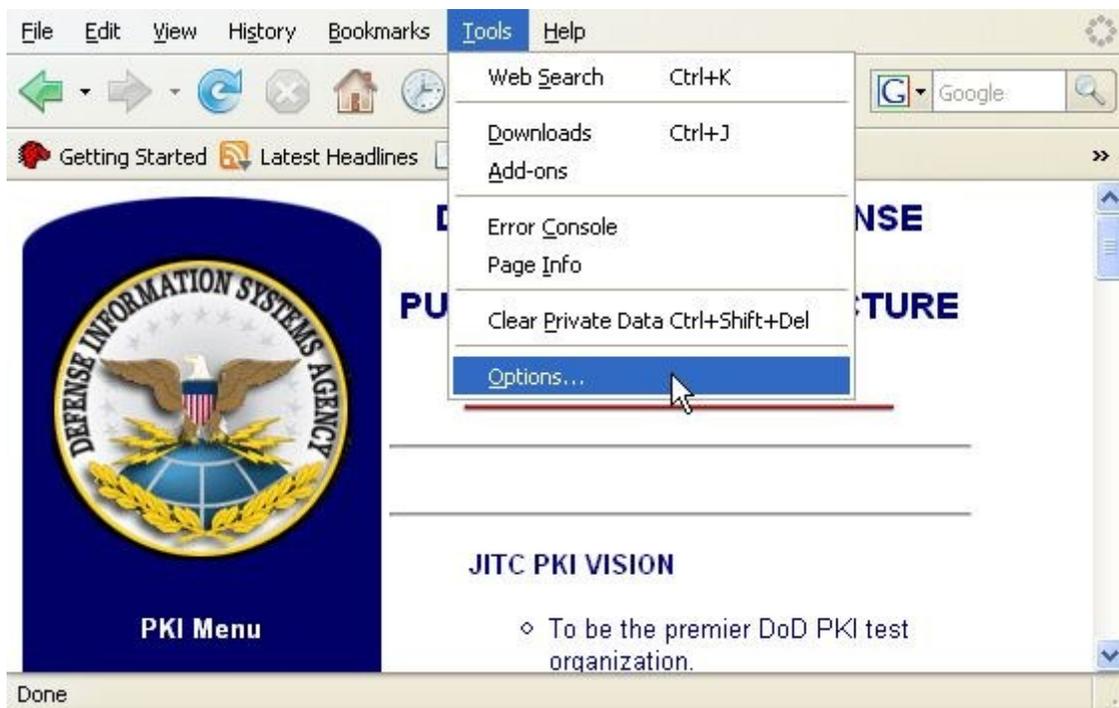
- 4) Click the **Install** button and wait for the installation to complete. Please wait until you see a confirmation dialog indicating the tool is finished.

## Using Common Access Card (CAC) certificates in Firefox

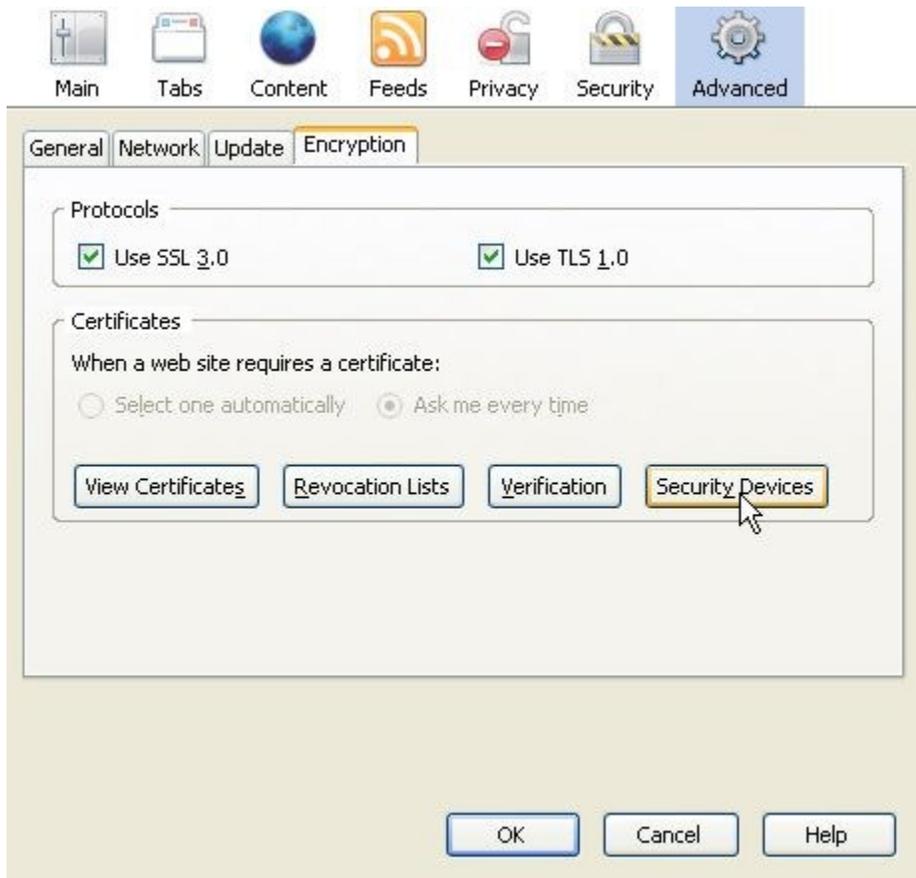
These instructions will enable ActivIdentity's ActivClient software to work within Firefox. Before proceeding, try to ensure the latest version of ActivClient is installed by going to the ActivClient website to check the latest version. Before installing the latest version, please uninstall any previous versions of ActivClient.

As of version 6.2, ActivClient by default configures Firefox to accept the CAC certificates without any additional configuration. You may use the following instructions to verify that it has been installed properly. If using an older version of ActivClient, these instructions will assist with proper configuration.

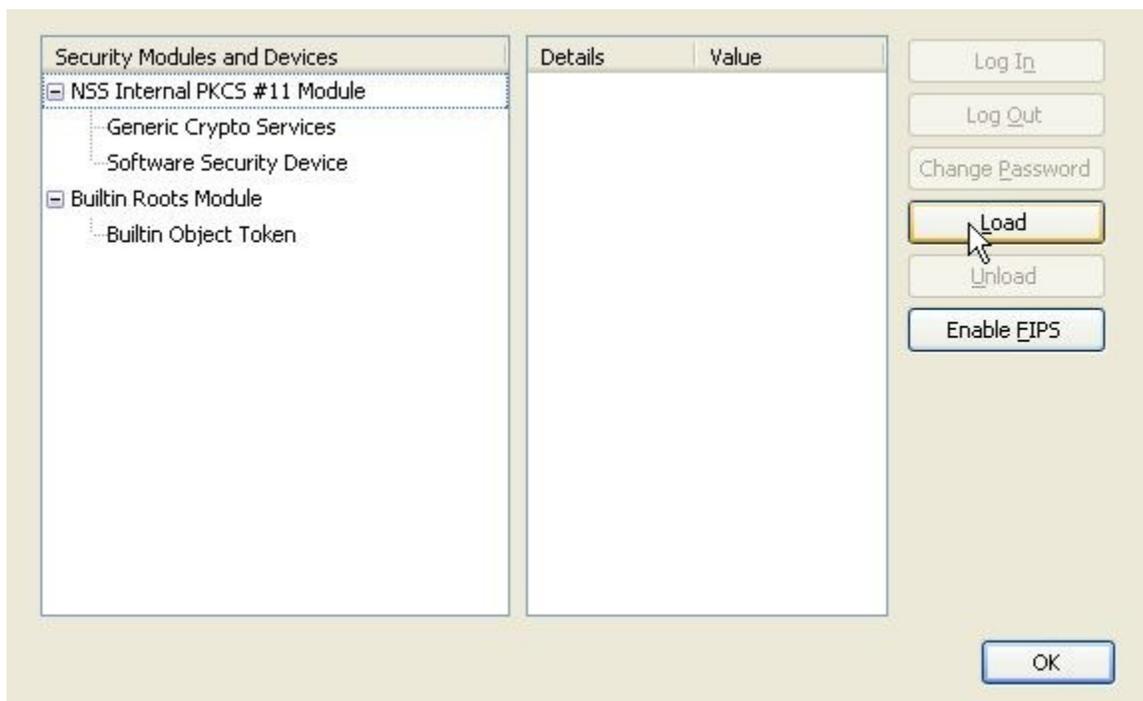
- 1) Open Firefox
- 2) Click on **Tools > Options** in the menu bar.



3) In the **Options** window, go to **Advanced** > **Encryption** > **Security Devices**.



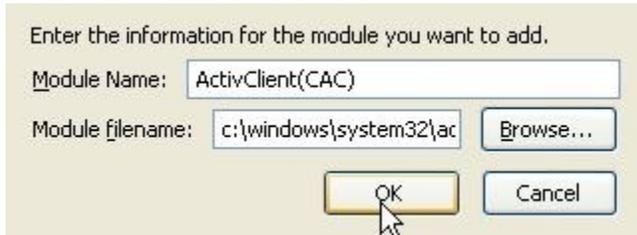
4) In the new window, click on **Load**.



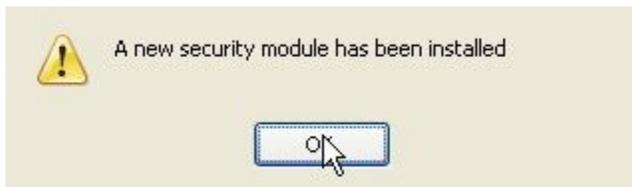
- 5) Enter "ActivClient(CAC)" for the **Module Name**.

Click **Browse** to the right of the **Module Filename** field. Browse to the location of the ActivClient PKCS11 library, acpkcs211.dll. This is typically located at C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll in ActivClient 6.2, and C:\Windows\system32\acpkcs201-ns.dll in ActivClient 6.1 and earlier.

Click **OK**, and then **OK** again in the confirmation window.



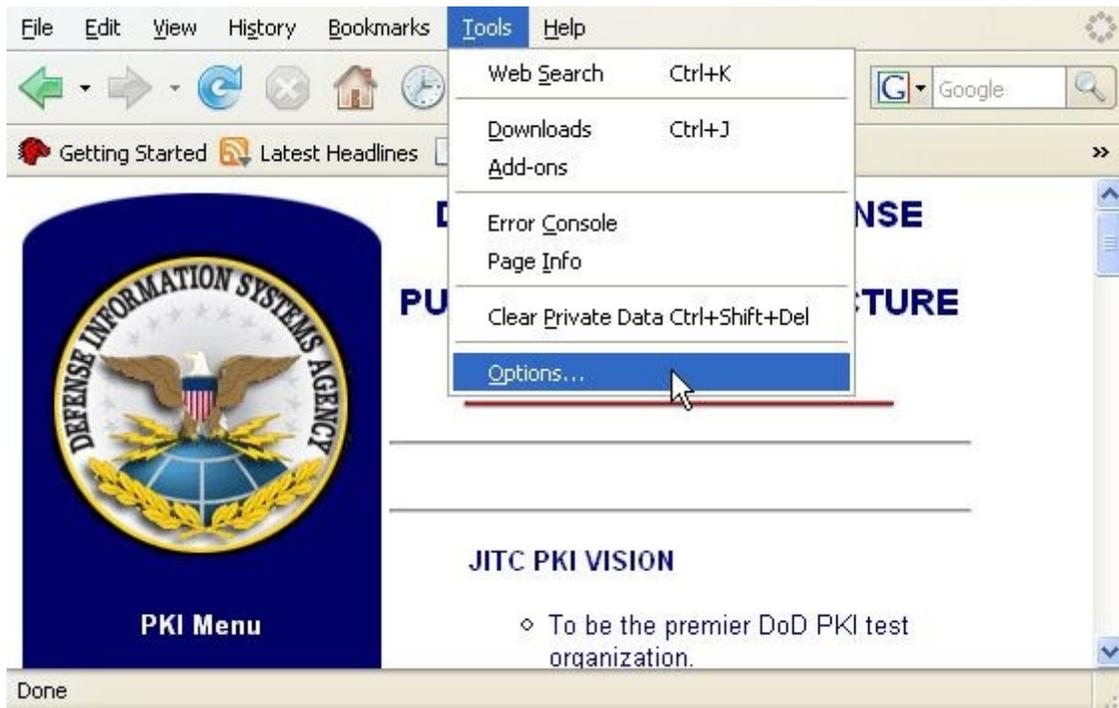
- 6) The confirmation message will show that the security device (CAC) was loaded. CAC certificates can now be used with the browser. Click **OK** to close the window.



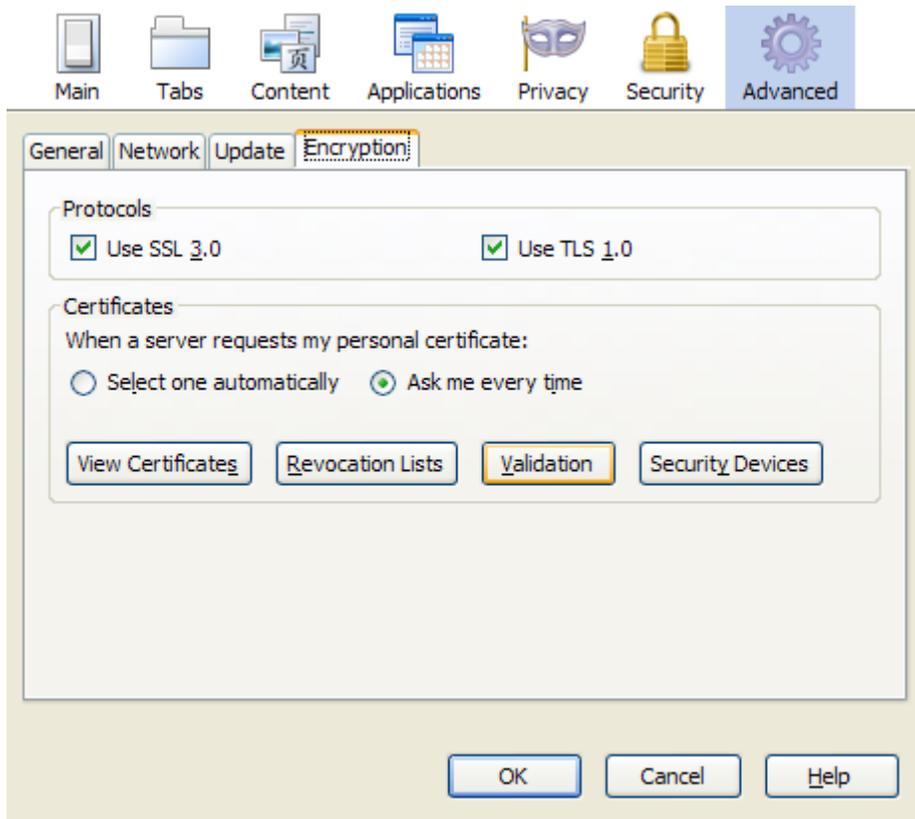
## Ensure the Online Certificate Status Protocol (OCSP) is Performing Revocation Checking

With any versions of ActivClient later than 6.2, these settings will be automatically configured. However, these instructions can be used to confirm proper configuration for older versions of ActivClient.

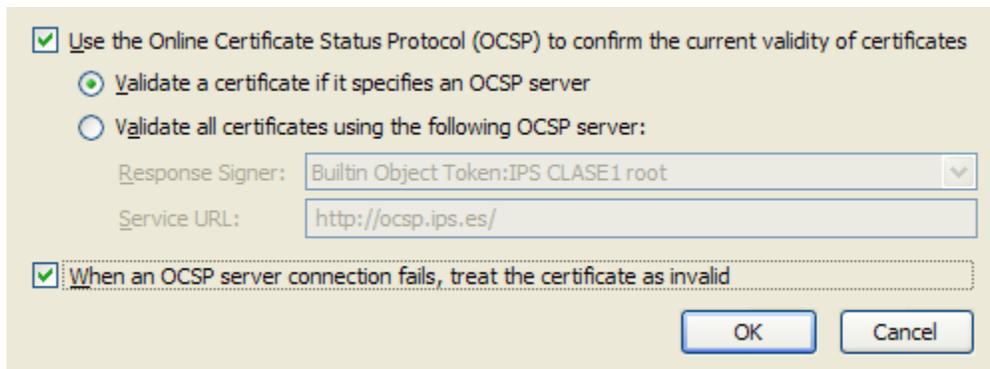
- 1) Open Firefox
- 2) Click on **Tools > Options** in the menu bar.



- 3) In the **Options** window, go to **Advanced > Encryption > Validation**.



- 4) Ensure the option **Use the OCSP to confirm the current validity of certificates** is checked. Also ensure **When an OCSP server connection fails, treat the certificate as invalid** is checked.



## Appendix A: Supplemental Information

### Website

Please visit the URL below for additional information

<http://iase.disa.mil/pki-pke>

### Technical Support

Contact technical support

[dodpke@mail.mil](mailto:dodpke@mail.mil)

### Acronyms

<b>CA</b>	Certificate Authority
<b>CAC</b>	Common Access Card
<b>NIPRNET</b>	Unclassified but Sensitive Internet Protocol Routing Network
<b>OCSP</b>	Online Certificate Status Protocol
<b>PKCS</b>	Public Key Cryptography Standard
<b>PKE</b>	Public Key Enablement
<b>PKI</b>	Public Key Infrastructure
<b>RG</b>	Reference Guide